Response to Department of Prime Minister and Cabinet
New Australian Government Data Sharing and Release Legislation
Issues Paper for Consultation
To: datalegislation@pmc.gov.au

1 August 2018

Response to Issues Paper

To whom it may concern

We refer to the New Australian Government Data Sharing and Release Legislation Issues Paper (**Issues Paper**) and the associated consultation meeting which took place in Sydney on Friday 27 July 2018 (**Sydney Consultation**) facilitated by Dr Phillip Gould, Assistant Secretary, Office of the National Data Commissioner (**NDC**).

This submission brings together the views of the following stakeholders:

- Melanie Marks, Principal, elevenM
- Susan Bennett, Principal Sibenco Legal & Advisory,
  Co-founder & Director, Information Governance ANZ
- Anna Johnston, Director, Salinger Privacy
- Professor Graham Greenleaf, Professor of Law & Information Systems, UNSW
- Professor Michael Adams, Professor of Corporate Law & Governance, Western Sydney University
- Associate Professor Thalia Anthony, Indigenous Law Centre, University of Technology Sydney
- Matthew Golab, Advisory Board Member Information Governance ANZ
- Katherine Sainty, Managing Director, Sainty Law
- Michele Bahari, CIPP/E, Admitted lawyer of the Supreme Court of NSW
- Shane Tully, Fellow of the Institute of Information Security Professionals (IISP)
- Nicole Vasin, General Counsel
- Tim de Sousa, Principal, elevenM
- James Logan, Senior Security Consultant, Aleron Security

Opening statement

We recognise that access to data drives efficiencies and advancements, and applied to the right purposes, with the right controls, can drive public benefits and positive societal outcomes. In some circumstances, it may be necessary and beneficial for identifiable information to be shared across government portfolios (for example, to minimise fraud).

We agree with the statements that "*Greater use and sharing of public data facilitates increased economic activity and improves productivity. Without improving data accessibility within government, the opportunity for enhanced productivity, increased competition, improved service delivery and research outcomes will be missed.*" (Issues Paper, page 3). However, the pursuit of greater data use and data sharing should not come at the cost of personal privacy and the freedoms that Australians enjoy today. We are concerned that the framework fails to consider the social impacts that it will enable. Significant clarification and debate is required before the framework should be accepted.

We advocate for a strictly controlled data sharing framework, justified by genuine public interest (and a 'no-harm' test), with strong oversight and personal choice for Australian citizens who wish to opt in or opt out. The My Health Record system debate which has dominated the press over the last fortnight clearly demonstrates that Australians want genuine choice and control when it comes to sharing their data.

The approach of overriding all existing secrecy provisions unless explicitly excluded is a simplistic and dangerous response to a complex problem. Existing laws reflect the evolution of hundreds of separate public policies, in each instance resulting from consultation and debate concerning their specific social and other impacts. The top down approach of this framework fails to make appropriate, contextual consideration of whether impacts are justified.

Our specific feedback is set out below.

Procedural issues: Consultation

1. There has been a lack of genuine public engagement and consultation undertaken by PM&C in relation to the proposed policy framework and supporting legislation, considering that it is purported to introduce the Data Sharing and Release Bill (**DS&R Bill**) within the next few months.

2. For a matter of such significance to Australian society, the consultation period has been too short to enable people to respond, and poorly communicated. We represent an engaged group of individuals, familiar with these matters of public policy, yet have had to rely on professional networks to inform us of this consultation, as it has not been widely publicised, even amongst interested stakeholder groups. We question therefore how the consultation outcomes will reflect the views of a cross-section of the Australian community.

3. The Issues Paper does not give adequate clarity or weight to the following facts:

   (i) That the framework may enable the sharing of *personal information*, not just de-identified information.

   (ii) That the framework may permit participation in data sharing by the private sector, even for commercial purposes.

   At the Sydney Consultation it was noted that these two settings remain open to consideration.

   These issues radically change what is proposed and expand the privacy risks associated with this policy initiative. The Issues Paper does not address these settings in a clear way.

4. It is similarly unclear how the Consumer Data Right (**CDR**) is proposed to interact with the DS&R Bill (if at all). An effective CDR may offset many of the privacy risks inherent in the data sharing framework by giving individuals the right to choose to share their data with trusted recipients only for the purposes that they have authorised. Whilst we acknowledge that the two frameworks are being developed by different portfolios, the impact of the DS&R Bill cannot be considered in isolation from the CDR.

Definitions

5. The Issues Paper lacks key definitions including 'data', 'safe', 'share' and 'release'.

Privacy is disregarded

6. At a fundamental level, the proposed Bill fails to provide any protections for individuals' privacy. Key principles of the Bill must emphasise the protection of privacy and protection of data.

7. We cannot give much weight to the statement in the Issues Paper (page 10) that safeguards legislated in the DS&R Bill would exist alongside those in the *Privacy Act.* The framework itself is a carve out from the general principle under Australian Privacy Principle 6 (under the *Privacy Act 1988*) that personal information must not be used for secondary purposes. At the Sydney Consultation, Dr Gould stated that sharing information under this framework would become an authorised exception under the Privacy Act. Presumably what was meant by this was that use or disclosure for a secondary purpose would be permitted under APP 6.2(b) "… *authorised by or under an Australian law*." This is a significant relaxation of APP 6 as it applies to government agencies (and potentially the private sector, as noted above).

8. At an operational level, it is unclear how key mechanisms for managing privacy risk (such as Privacy Impact Assessments which are a requirement for agencies under the *Privacy (Australian Government Agencies — Governance) APP Code 2017*) would operate in conjunction with the DS&R Bill.

9. It is proposed that guidance on the Five Safes will be developed by the NDC in consultation with relevant agencies including the Office of the Australian Information Commissioner (**OAIC**) to appropriately address privacy risks (page 15). The management of privacy risk should be addressed in legislation, not guidance. Further, noting that the principles of the Bill fail to consider privacy at all, it is inappropriate for the NDC to develop guidance on how to address privacy risks. Funding should be allocated to the OAIC to develop any guidance.

10. Creating a new channel for data sharing/release just complicates matters more; why not reform ss.95 and 95A of the *Privacy Act 1988* instead (which the Productivity Commission also recommended[1]) to broaden out the categories of data that can be shared for research purposes, and broaden out the allowable research purposes? Any non-personal information datasets (data about the environment etc.) can then be dealt with under the new Bill.

11. Further, as stated above, the approach of overriding all existing secrecy provisions unless explicitly excluded is a simplistic and dangerous response to a complex problem. Instead of the top down approach of this framework, we advocate for a more nuanced approach, to ensure appropriate, contextual consideration of whether impacts are justified in each case. An alternate approach would be to commence a project to carefully review each of the 175 statutes with secrecy provisions, with a plan to insert a standard exemption pointing to the DS&R Act and/or the research exemptions in the Privacy Act, if deemed appropriate for that

[1] Recommendation 6.16 in Productivity Commission, *Inquiry Report: Data Availability and Use*, No. 82, 31 March 2017

statute after due consultation and consideration. See also ALRC recommendations for review and guidance of secrecy offences.

De-identified data

12. There is a misplaced faith in the safety of 'de-identified' data. The recent breach of the Privacy Act by the Department of Health regarding the release of supposedly de-identified MBS/PBS data offers a case in point. It is also quite possible to identify a person via metadata (see for example, this study by University College, London).

13. The standard for 'safe' data release should be set to the higher test of 'anonymous' data, rather than 'de-identified' data. The new European law the *General Data Protection Regulation* adopts the higher standard of 'anonymous' data, reflecting a lower risk appetite towards re-identification risk than the Australian Privacy Act currently allows. We note that the Office of the Victorian Information Commissioner **(OVIC)** has recently advocated that the risks of re-identification are so high that personal information should never be publicly released in unit level record form – see 'Protecting unit-record level personal information - The limitations of de-identification and the implications for the Privacy and Data Protection Act 2014' **(OVIC Report).**

Five Safes is not a complete risk management approach

14. The Five Safes is a conceptual approach to thinking about data access risks. It doesn't address all the issues.

15. For a risk management approach to be consistent and effective, there must be a common understanding of risk tolerance (i.e. what constitutes 'safe'?). The proposed framework puts the onus of assessing risk on the data custodian. We believe that the framework requires a statement of risk tolerance/appetite which has the mandate of the Australian community, flexes to the sensitivity of the dataset and includes a 'no-harm' test. The initial and evolving risk appetite statement must be set by appropriate bodies in consultation with the Australian community.

16. The Issues Paper states that data custodians will be responsible for applying the principles and requirements of the DS&R Bill to share and release data appropriately (page 18). How will agencies (or other custodians) be equipped to make these risk-based decisions? Agencies will need to hold not only a clear and accurate understanding of the framework but also a very detailed understanding of each proposed application of the data in order to make a sound determination. The resources required to exercise effective, risk-based decision making may be prohibitive for agencies and other participants, leading agencies not to use the framework, or to make poor decisions.

17. The Five Safes methodology tests for risks in relation to identity disclosure. It is not a risk assessment method for determining other types of privacy risks such as attribute disclosure or individuation.

18. The Five Safes methodology helps to determine *how* to share data safely. It does not assess *whether* the data should be shared or released at all. We advocate that each project should be subject to a public interest test and a 'no harm' test. Also, in every instance, proposed sharing or disclosure should be subject to examination of whether the project would breach

privacy promises made to individuals in the past or would be within their expectations. This is a practical way of establishing that the initiative has a 'social licence'.

Risk management requires effective controls

19. It is not clear who will be responsible for ensuring the adequacy and implementation of controls. Will it be the data custodian – and if so, again, how are they resourced and equipped to do so? Will it be the DCO? At the Sydney Consultation, Dr Gould noted that the NDC's Office would be staffed by 18-20 full time employees. The Issues Paper notes (page 8): "*The Bill will ensure data is shared for the right purposes, with risks appropriately managed.*" Accountability for controls assurance must be established in legislation.

20. In the case of financial information risk management, the assurance process is based on independently set audit standards against which the entity is compelled by law to be audited by independent, qualified auditors. Given that personal information is now considered to be an asset of most organisations, it should be afforded a similar level of ex ante protection.

Governance

21. At a fundamental level, it is not sufficient for the NDC to have powers to investigate or suspend activities at all given that its role is to 'champion greater data sharing and release', (page 20), whatever the approach. This would present conflict in the strategic direction of the NDC.

22. As to privacy oversight specifically, we are concerned about inadequate funding for an appropriate regulatory body to oversee privacy aspects of the framework. Putting aside the issue of conflict, the NDC has a huge initiative to deliver with limited headcount, as detailed above. Given that privacy protection does not appear in the principles of the Bill nor the responsibilities of the NDC, it is hard to see how the NDC's limited funding will enable it to provide any meaningful oversight of privacy aspects of the framework. This accountability should reside with the OAIC, bolstered by additional funding.

23. Accredited Data Authorities (ADAs) must be properly qualified to identify and manage privacy risk as part of assessing a proposed data sharing or release arrangement. For example, ADAs must be equipped to identify the risk of harm to individuals in all contexts enabled by the legislation.

Penalty framework takes the wrong angle

24. The Issues Paper only ever mentions 'consequences' (by and large unspecified) arising from the DSR scheme, and does not mention liability. To the contrary, it proposes an immunity against criminal liability for any data custodians acting 'in good faith with a genuine belief that disclosure is required or permitted under the DS&R Bill' (page 21). It is easy to see this morphing into a more general immunity for any civil liability which might arise from harmful consequences (including interferences with privacy but not limited to them) resulting from DS&R activities that go wrong (such as the notorious Open Data release of Medicare data which Melbourne researchers showed not to be 'de-identified' – see **OVIC Report**).

25. The Issues Paper should have proposed the opposite: (i) all uses of data consequent upon activities approved under the DS&R legislation should attract absolute legal liability for any harm caused to individuals (a real 'no harm' principle), or at the least legal liability for any negligent actions by any party involved; and (ii) unless absolute liability is enacted, the ALRC recommendations for a 'serious invasions of privacy' should be enacted, with negligent release or use of government data being specifically listed in the legislation. Individuals harmed need access to the courts, and class actions.

26. We support the DS&R Bill giving the NDC powers to penalise non-compliance, such as intentional misuse of data (page 21). However, we consider that it more likely that harm for individuals will result from poor decision making – for instance, an assessment of risk which fails to identify the risk of harm to vulnerable sectors of the community, a de-identification process which is inadequate, leading to harm through re-identification, or controls that are inadequate or not implemented adequately. None of these examples are risks of non-compliance, and yet they give rise to real risks of harm for individual Australians. The legislation must address these risks.

Purposes as defined are too broad

27. Within the proposed framework, the threshold for release or sharing of data is too low because the purposes are too broad, particularly given that the framework contemplates the sharing of personal information (not just deidentified information). For example, there are very few activities of agencies that would not be caught by the terms "inform government policy making" or "support the efficient delivery of government services or government operations". The term "administering or enforcing compliance requirements" is equally broad. Accordingly, the purposes test should provide that in every instance the public interest must be met and a 'no-harm' test must be passed.

28. During the Sydney Consultation, Dr Gould referred to the data sharing laws of various States and Territories (who may also sign on to the framework) and noted that some jurisdictions have introduced laws prohibiting data usage to target or intervene with an individual. We support the addition of this higher threshold into the Commonwealth framework.

We welcome the publication of data sharing arrangements

29. We support the proposal that the DS&R Bill would provide for data sharing agreements to be publicly available.

30. Data sharing agreements involving personal information (whether or not attempts have been made to de-identify the personal information) should be required to address compliance with the APPs including in relation to data security, data quality, retention and destruction, access and correction. They should include a right to inspection or audit of the recipient of the data by the OAIC and/or the supplier of the data.

Signed by the following:

Name

Melanie Marks
Principal, elevenM
Email: hello@elevenm.com.au

Susan Bennett
Principal, Sibenco Legal & Advisory
Co-founder & Director, Information Governance ANZ
Email: susan.bennett@sibenco.com

Anna Johnston
Director, Salinger Privacy

Professor Graham Greenleaf
Professor of Law & Information Systems
University of New South Wales

Professor Michael Adams
Professor of Corporate Law and Governance
Western Sydney University

Associate Professor Thalia Anthony
Indigenous Law Centre
University of Technology Sydney

Matthew Golab
Advisory Board Member, Information Governance ANZ

Katherine Sainty
Managing Director, Sainty Law

Michele Bahari
CIPP/E, Admitted lawyer of the Supreme Court of NSW

Shane Tully
Fellow of the Institute of Information Security Professionals

Nicole Vasin
General Counsel

Tim de Sousa
Principal, elevenM

James Logan
Senior Security Consultant, Aleron Security